

*Уважаемые читатели! Не удивляйтесь, что эта книга начинается с восьмой главы. Авторы разделили свой труд на две части. Первая часть книги вышла в издательстве «Питер» в 2013 году. В ней рассмотрены следующие темы:*

- Глава 1.** Общие представления и инструментальные средства
- Глава 2.** Архитектура системы
- Глава 3.** Системные механизмы
- Глава 4.** Механизмы управления
- Глава 5.** Процессы, потоки и задания
- Глава 6.** Безопасность
- Глава 7.** Сеть

# Оглавление

<b>Введение .....</b>	<b>15</b>
<b>Глава 8. Подсистема ввода-вывода .....</b>	<b>21</b>
Компоненты подсистемы ввода-вывода .....	21
Диспетчер ввода-вывода .....	24
Стандартная обработка ввода-вывода .....	24
Драйверы устройств .....	26
Типы драйверов устройств .....	26
WDM-драйверы .....	27
Многоуровневые драйверы .....	27
Структура драйвера .....	32
Объекты драйверов и устройств .....	35
Открытие устройств .....	40
Обработка ввода-вывода .....	47
Типы ввода-вывода .....	47
Синхронный и асинхронный ввод-вывод .....	47
Быстрый ввод-вывод .....	48
Ввод-вывод для файлов, отображенных на память, и кэширование файлов .....	49
Фрагментированный ввод-вывод .....	50
Пакеты запросов на ввод и вывод .....	50
Блоки стека IRP-пакетов .....	52
Управление буфером IRP-пакетов .....	54

Запрос ввода-вывода к одноуровневому драйверу .....	55
Обработка прерывания .....	57
Завершение обработки запроса на ввод-вывод .....	59
Синхронизация .....	61
Запросы ввода-вывода к многоуровневым драйверам .....	62
Независимый от программных потоков ввод-вывод .....	69
Отмена ввода-вывода .....	70
Отмена ввода-вывода, инициированная пользователем .....	71
Отмена ввода-вывода при завершении программного потока .....	72
Порты завершения ввода-вывода .....	74
Объект IoCompletion .....	75
Применение портов завершения .....	75
Функционирование порта ввода-вывода .....	77
Определение приоритетов ввода-вывода .....	80
Приоритеты ввода-вывода .....	80
Стратегии выбора приоритета .....	80
Предотвращение инверсии приоритетов ввода-вывода (наследование приоритетов ввода-вывода) .....	83
Повышение и понижение приоритетов ввода-вывода .....	84
Резервирование полосы пропускания (планирование файлового ввода-вывода) ..	86
Уведомления о сеансах .....	87
Программа Driver Verifier .....	87
Среда KMDF .....	90
Структура и функциональность KMDF-драйвера .....	90
Модель данных в KMDF .....	92
Модель ввода-вывода в KMDF .....	97
Среда UMDF .....	100
PnP-диспетчер .....	104
Уровень поддержки технологии Plug and Play .....	105
Поддержка технологии Plug and Play со стороны драйвера .....	105
Загрузка, инициализация и установка драйвера .....	107
Параметр Start .....	108
Перечисление устройств .....	109
Стеки устройств .....	113
Загрузка драйверов для стека устройств .....	114
Установка драйвера .....	119
Диспетчер электропитания .....	123
Работа диспетчера электропитания .....	125
Участие драйверов в управлении электропитанием .....	126
Управление электропитанием устройств со стороны драйверов и приложений .....	130
Запросы на изменение режима электропитания .....	130
Управление электропитанием со стороны центрального процессора .....	133
Политики парковки ядер .....	134
Функция полезности .....	135
Переопределение алгоритма .....	138
Увеличение/уменьшение числа запаркованных ядер .....	139

Пороговые значения и варианты настройки политик .....	139
Проверка производительности .....	143
Заключение .....	149
<b>Глава 9. Управление внешней памятью .....</b>	<b>151</b>
Базовая терминология .....	151
Дисковые устройства .....	152
Вращающиеся магнитные диски .....	152
Формат сектора диска .....	152
Твердотельные диски .....	154
Флэш-память типа NAND .....	155
Удаление файлов и команда Trim .....	156
Драйверы дисков .....	158
Программа Winload .....	158
Драйверы дисковых класса, порта и мини-порта .....	159
iSCSI-драйверы .....	160
MPIO-драйверы .....	161
Объекты устройств для дисков .....	163
Диспетчер разделов .....	165
Управление томами .....	166
Базовые диски .....	166
Схема MBR .....	166
Схема GPT .....	167
Диспетчер томов на базовых дисках .....	168
Динамические диски .....	169
База данных для LDM .....	169
Разбиение на разделы в стиле LDM и GPT или в стиле MBR .....	173
Диспетчер томов для динамических дисков .....	174
Управление составными томами .....	175
Перекрытые тома .....	175
Чередующиеся тома .....	176
Зеркальные тома .....	177
RAID-5 .....	179
Пространство имен томов .....	180
Диспетчер монтирования .....	181
Точки монтирования .....	182
Монтирование томов .....	183
Ввод и вывод на томах .....	187
Служба виртуальных дисков .....	188
Поддержка виртуального жесткого диска .....	190
Присоединение виртуальных жестких дисков .....	191
Вложенные файловые системы .....	192
Шифрование диска BitLocker .....	192
Ключи шифрования .....	194
Доверенный платформенный модуль .....	197
Процесс загрузки BitLocker .....	200

Восстановление с помощью BitLocker .....	201
Драйвер шифрования всего тома .....	202
Управление системой BitLocker .....	204
Технология BitLocker To Go .....	205
Служба теневого копирования томов .....	207
Теневые копии .....	207
Полные теневые копии .....	207
Разностные теневые копии .....	207
Архитектура VSS .....	208
Функционирование VSS .....	208
Провайдер теневого копирования .....	210
Применение в Windows .....	212
Резервное копирование .....	212
Предыдущие версии и восстановление системы .....	213
Заключение .....	216
<b>Глава 10. Управление внутренней памятью .....</b>	<b>217</b>
Знакомство с диспетчером памяти .....	217
Компоненты диспетчера памяти .....	218
Внутренняя синхронизация .....	219
Исследование использования памяти .....	220
Службы диспетчера памяти .....	224
Большие и малые страницы .....	224
Резервирование и подтверждение страниц .....	227
Лимит подтверждения .....	230
Блокирование памяти .....	231
Гранулярность выделения памяти .....	231
Совместно используемая память и отображаемые файлы .....	232
Защита памяти .....	235
Защита страниц от выполнения .....	237
Программное предотвращение выполнения кода .....	242
Копирование при записи .....	244
Оконные расширения адресов .....	245
Кучи режима ядра .....	248
Размеры пулов .....	249
Мониторинг использования пулов .....	251
Ассоциативные списки .....	255
Диспетчер кучи .....	257
Типы куч .....	257
Структура диспетчера кучи .....	258
Синхронизация кучи .....	259
Слабо фрагментированная куча .....	260
Механизмы безопасности куч .....	261
Средства отладки куч .....	262
Инструмент pageheap .....	263
Отказоустойчивая куча .....	264
Структуры виртуального адресного пространства .....	265

Структура адресных пространств на платформе x86 .....	267
Структура системного адресного пространства на платформе x86. ....	270
Пространство сеанса на платформе x86. ....	270
Записи системной таблицы страниц. ....	273
Структура адресных пространств 64-разрядных систем .....	274
Ограничения виртуальной адресации на платформе x64. ....	278
16-терабайтное ограничение для Windows на платформе x64 .....	278
Динамическое управление системным виртуальным адресным пространством .....	281
Квоты системного виртуального адресного пространства .....	284
Структура пользовательского адресного пространства .....	286
Рандомизация образа .....	288
Рандомизация стека. ....	290
Рандомизация кучи. ....	290
ASLR в адресном пространстве ядра .....	290
Управление средствами смягчения уровня опасности .....	290
Преобразование адресов .....	292
Преобразование виртуальных адресов на платформе x86 .....	292
Каталоги страниц .....	296
Таблицы страниц и их записи. ....	297
Сравнение аппаратного и программного битов записи .....	299
Байт внутри страницы .....	300
Буфер быстрого преобразования адресов .....	300
Расширение физических адресов. ....	302
Преобразование виртуальных адресов на платформе x64 .....	306
Преобразование виртуальных адресов на платформе IA64 .....	308
Обработка ошибок отсутствия страниц .....	309
PTE-записи .....	310
Прототипные PTE-записи .....	312
Страничный ввод-вывод .....	315
Конфликтные ошибки отсутствия страниц .....	315
Кластерные ошибки отсутствия страниц. ....	316
Страничные файлы .....	318
Показатель подтверждения и системный лимит подтверждения. ....	319
Показатель подтверждения и размер страничного файла .....	323
Стеки. ....	325
Пользовательские стеки .....	326
Стеки ядра .....	327
DPC-стек .....	328
Дескрипторы виртуальных адресов .....	328
Дескрипторы виртуальных адресов процесса .....	329
Чередующиеся дескрипторы виртуальных адресов .....	331
NUMA .....	331
Объекты разделов .....	333
Программа проверки драйверов. ....	340
База данных номеров страничных блоков .....	345
Динамика списков страниц .....	349

Приоритеты страниц .....	359
Подсистема записи измененных страниц .....	362
Структура данных PFN-записи .....	364
Лимиты физической памяти .....	370
Лимиты памяти клиентских версий Windows .....	371
Фактические лимиты памяти на 32-разрядных клиентских системах .....	372
Рабочие наборы .....	375
Подкачка по требованию .....	375
Компонент логической предвыборки .....	376
Политика размещения .....	380
Управление рабочими наборами .....	381
Диспетчер настройки баланса и поток подкачки .....	385
Системные рабочие наборы .....	386
События уведомлений в памяти .....	387
Упреждающее управление памятью (супервыборка) .....	390
Компоненты .....	390
Трассировка и протоколирование .....	393
Сценарии .....	394
Приоритеты страниц и переконфигурирование .....	395
Устойчивое функционирование .....	397
Служба ReadyBoost .....	400
Технология ReadyDrive .....	402
Унифицированное кэширование .....	402
Отражение процессов .....	405
Заключение .....	409
<b>Глава 11. Диспетчер кэша .....</b>	<b>410</b>
Основные возможности диспетчера кэша .....	410
Единый централизованный системный кэш .....	411
Диспетчер памяти .....	411
Согласованность кэша .....	412
Кэширование виртуальных блоков .....	413
Кэширование на основе потоков данных .....	414
Поддержка самовосстанавливающихся файловых систем .....	414
Управления виртуальной памятью кэша .....	415
Размер кэша .....	417
Виртуальный размер кэша .....	417
Размер рабочего набора кэша .....	418
Физический размер кэша .....	419
Структуры данных кэша .....	421
Общесистемные структуры данных кэша .....	422
Структуры данных кэша, относящиеся к каждому файлу .....	425
Интерфейсы файловых систем .....	431
Копирование в кэш и из кэша .....	432
Кэширование через интерфейсы отображения и фиксации .....	432
Кэширование через интерфейсы прямого доступа к памяти .....	433

Быстрый ввод-вывод .....	433
Упреждающее чтение и отложенная запись .....	435
Интеллектуальное упреждающее чтение .....	436
Кэширование с обратной записью и отложенная запись .....	437
Отключение режима отложенной записи для файла .....	445
Принудительное включение в кэше режима сквозной записи на диск .....	445
Сброс отображаемых файлов .....	445
Ограничение записи .....	446
Системные программные потоки .....	448
Заключение .....	449
<b>Глава 12. Файловые системы .....</b>	<b>450</b>
Форматы файловых систем в Windows .....	451
CDFS .....	451
UDF .....	452
FAT12, FAT16 и FAT32 .....	452
exFAT .....	456
NTFS .....	456
Архитектура драйверов файловой системы .....	457
Локальные FSD-драйверы .....	458
Удаленные FSD-драйверы .....	459
Блокировка .....	461
Работа файловой системы .....	467
Явный ввод-вывод .....	468
Подсистема записи модифицированных и отображенных страниц .....	472
Подсистема отложенной записи .....	473
Программный поток опережающего чтения .....	473
Обработчик ошибок страниц .....	474
Фильтрующие драйверы файловой системы .....	474
Программа Process Monitor .....	474
Решение проблем файловой системы .....	476
Базовый и расширенный режимы программы Process Monitor .....	476
Устранение неисправностей с помощью Process Monitor .....	477
Файловая система с типовым протоколированием .....	478
Марширование .....	478
Типы журналов .....	479
Структура журнала .....	481
Регистрационные номера транзакций в журнале .....	482
Блоки журнала .....	483
Страницы владельца .....	484
Преобразование виртуальных LSN-номеров в физические .....	485
Политики управления .....	486
Цели разработки и особенности NTFS .....	487
Требования к профессиональной файловой системе .....	487
Восстанавливаемость .....	487
Безопасность .....	487

Избыточность данных и отказоустойчивость .....	488
Нетривиальные возможности NTFS .....	488
Множественные потоки данных .....	489
Имена на базе Unicode .....	491
Универсальный механизм индексации .....	491
Динамическое переназначение поврежденных кластеров .....	492
Жесткие ссылки .....	492
Символические (мягкие) ссылки и соединения .....	493
Сжатие и разреженные файлы .....	495
Протоколирование изменений .....	496
Квоты томов для пользователей .....	496
Отслеживание связей .....	498
Шифрование .....	498
Поддержка POSIX .....	499
Дефрагментация .....	499
Динамическое разбиение на разделы .....	501
Драйвер файловой системы NTFS .....	502
NTFS-структура на диске .....	505
Томы .....	505
Кластеры .....	506
Главная таблица файлов .....	507
Индексы файловых записей .....	511
Файловые записи .....	511
Имена файлов .....	514
Резидентные и нерезидентные атрибуты .....	518
Сжатие данных и разреженные файлы .....	521
Сжатие разреженных данных .....	522
Сжатие неразреженных данных .....	524
Разреженные файлы .....	526
Файл журнала изменений .....	526
Индексация .....	529
Идентификаторы объектов .....	531
Отслеживание квот .....	531
Консолидированная система безопасности .....	533
Точки повторной обработки .....	535
Поддержка транзакций .....	535
Изоляция .....	536
Транзакционные API-интерфейсы .....	538
Диспетчеры ресурсов .....	539
Реализация на диске .....	541
Реализация протоколирования .....	543
Реализация восстановления .....	543
Поддержка восстановления в NTFS .....	544
Техническое решение .....	545
Протоколирование метаданных .....	546
Служба файла журнала .....	546



Типы записей журнала .....	548
Восстановление .....	551
Анализ .....	551
Повторение .....	552
Отмена .....	553
Восстановление поврежденных кластеров в NTFS .....	555
Самовосстановление .....	559
Безопасность в шифрующей файловой системе .....	560
Первое шифрование файла .....	563
Шифрование файловых данных .....	564
Процесс дешифрирования .....	565
Резервное копирование шифрованных файлов .....	566
Копирование зашифрованных файлов .....	567
Заключение .....	567
<b>Глава 13. Запуск и завершение работы системы .....</b>	<b>568</b>
Процесс загрузки .....	568
Начальные этапы загрузки систем на базе BIOS .....	568
Загрузочный сектор систем на базе BIOS и Bootmgr .....	572
Загрузка в UEFI-системах .....	587
Загрузка с iSCSI-устройств .....	588
Инициализация ядра и исполнительных подсистем .....	589
Smss, Csrss и Wininit .....	597
ReadyBoot .....	603
Автоматически запускаемые образы .....	603
Анализ проблем при загрузке и запуске системы .....	605
Последняя удачная конфигурация .....	605
Безопасный режим .....	605
Загрузка драйверов в безопасном режиме .....	606
Программы с поддержкой безопасного режима .....	608
Протоколирование загрузки в безопасном режиме .....	608
Среда восстановления Windows .....	609
Решение распространенных проблем загрузки .....	613
Повреждение MBR .....	613
Повреждение загрузочного сектора .....	614
Неправильная конфигурация BCD .....	614
Повреждение системных файлов .....	615
Повреждение куста System .....	617
Сбой или зависание после вывода экранной заставки .....	617
Завершение работы .....	619
Заклучение .....	622
<b>Глава 14. Анализ аварийного дампа .....</b>	<b>623</b>
Почему в Windows случаются сбои? .....	623
Синий экран .....	624
Причины сбоев в Windows .....	625

Устранение проблем при сбоях .....	627
Файлы аварийного дампа .....	629
Генерация аварийного дампа .....	635
Передача в Microsoft отчетов об ошибках .....	638
Анализ сбоев через Интернет .....	639
Базовый анализ аварийного дампа .....	640
Программа Notmyfault .....	641
Базовый анализ .....	642
Детальный анализ .....	643
Инструменты устранения сбоев .....	645
Переполнение буфера, повреждение памяти и особый пул .....	646
Перезапись кода и защита системного кода от записи .....	649
Углубленный анализ аварийных дампов .....	651
Засорение стека .....	652
Зависание, или отсутствие отклика .....	654
Если аварийный дамп отсутствует .....	659
Анализ распространенных стоп-кодов .....	662
Код 0xD1 — DRIVER_IRQL_NOT_LESS_OR_EQUAL .....	662
Код 0x8E — KERNEL_MODE_EXCEPTION_NOT_HANDLED .....	664
Код 0x7F — UNEXPECTED_KERNEL_MODE_TRAP .....	665
Код 0xC5 — DRIVER_CORRUPTED_EXPOOL .....	667
Отказы аппаратуры .....	670
Заключение .....	671
<b>Об авторах .....</b>	<b>672</b>